ATTACHMENT A
Device to be Searched

This warrant applies to the following cellphone ("**SUBJECT TELEPHONE**") that **is** currently stored in the custody of the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") in Baltimore, Maryland:

a. A black UMX model U693CL cellular phone, with FCC ID: P46-U693CL and serial number 693CL60421010998, recovered from Terrence HILLMAN, on August 12, 2021, currently in the custody of the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF") in Baltimore, Maryland ("**SUBJECT TELEPHONE**")

ATTACHMENT B
Items to be Seized

All records contained in the item described in Attachment A which constitute evidence of violations of 18 U.S.C. § 922(g)(1) Possession of a Firearm by a Prohibited Person, including but not limited to that outlined below:

1. All evidence of firearms possession; distribution; and co-conspirators and/or associations to same.

2. Contact logs that refer or relate to the user of any and all numbers on the Subject Electronic Devices.

3. Call logs reflecting date and time of received calls.

4. Any and all digital images and videos of people associated with this investigation.

5. Text messages to and from the **SUBJECT TELEPHONE** that refer or relate to the crimes under investigation.

6. Records of incoming and outgoing voice communications that refer or relate to the crimes under investigation.

7. Voicemails that refer or relate to the crimes under investigation.

8. Voice recordings that refer or relate to the crimes under investigation.

9. Any data reflecting the phone's location.

10. Contact lists.

11. Any and all records related to the location of the user(s) of the devices.

12. For the **SUBJECT TELEPHONE**:

a. Evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the Devices, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the **SUBJECT TELEPHONE** of other storage devices or similar containers for electronic evidence;

e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the Devices;

f. evidence of the times the **SUBJECT TELEPHONE** were used;

g. passwords, encryption keys, and other access devices that may be necessary to access the **SUBJECT TELEPHONE**;

h. documentation and manuals that may be necessary to access the Devices or to conduct a forensic examination of the **SUBJECT TELEPHONE**;

i. contextual information necessary to understand the evidence described in this attachment.

With respect to the search of any of the items described above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

1. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

2. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

3. "scanning" storage areas to discover and possible recover recently deleted files;

4. "scanning" storage areas for deliberately hidden files; or

5. performing key word searches or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

If after performing these procedures, the directories, files or storage areas do not reveal evidence of the specified criminal activity, the further search of that particular directory, file or storage area, shall cease.

With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privilege.